

MERCHANTS, DOSTAWCY I ISO

Transaction laundering: jak wykrywają go dostawcy i jak wpadają w niego uczciwi merchanti

Opublikowano 28 września 2026

Przetwarzanie płatności jednej firmy przez konto merchanta innej należy do najpoważniejszych naruszeń w płatnościach kartowych. Czym jest, jak wychodzi na jaw i jakie zwykłe praktyki go przypominają.

Transaction laundering to przetwarzanie płatności kartowych jednej firmy przez konto merchanta zatwierdzone dla innej firmy. Nazywa się to także factoringiem albo nieautoryzowaną agregacją. Posiadacz konta przeszedł ocenę ryzyka. Firma, która faktycznie przyjmuje pieniądze, jej nie przeszła i zwykle nie mogłaby przejść.

Dlaczego traktuje się to tak poważnie

Wszystko, co dostawca płatności wie o ryzyku, jest przypisane do merchanta, którego zatwierdził: co sprzedaje, komu, za ile i z jaką historią sporów. Gdy przez to konto przechodzi sprzedaż kogoś innego, nic z tego nie jest prawdą. Dostawca ponosi ryzyko, którego nigdy nie ocenił, i być może przekazuje pieniądze za coś nielegalnego.

Organizacje kartowe obarczają odpowiedzialnością agenta rozliczeniowego. Sprawa wykryta przez organizację oznacza kary dla agenta, zamknięcie konta merchanta i zwykle wpis na listę MATCH Mastercarda pod kodem launderingu, na który przymknie oko bardzo niewielu dostawców.

Jak wychodzi na jaw

Dostawcy i zatrudniane przez nich firmy monitorujące szukają rozbieżności między tym, do czego konto zostało zatwierdzone, a tym, co robi.

- **Monitoring strongy.** Roboty sprawdzają, czy zatwierdzona strona nadal sprzedaje to, co sprzedawała, i szukają innych stron korzystających z tej samej płatności, tej samej strony płatniczej albo tych samych identyfikatorów merchanta.

- **Wzorce transakcji.** Kwoty, godziny i kraje klientów niepasujące do zatwierdzonej działalności. Sklep z kawą nie przyjmuje o trzeciej nad ranem serii identycznych płatności na okrągłe kwoty z innego kontynentu.
- **Zakupy testowe.** Analitycy kupują na podejrzanych stronach i sprawdzają, przez które konto merchanta przychodzi obciążenie.
- **Treść sporów.** Posiadacz karty kwestionujący obciążenie często mówi, co naprawdę kupił. Gdy nie jest to coś, co merchant sprzedaje, dostawca to zauważa.
- **Dane o źródle wejścia i deskryptorze.** Strona, z której przyszedł klient, oraz deskryptor na wyciągu, który nie pasuje do żadnej zatwierdzonej strony.

Jak uczciwi merchanti uruchamiają te same alarmy

Większość firm wychwyconych przez te kontrole nie jest przykrywką dla niczego. Zrobiły coś zwyczajnego, nie mówiąc o tym dostawcy.

1. **Druga strona na tym samym koncie.** Nowa marka albo nowy sklep, rozliczany przez istniejącą płatność. Dla monitoringu niezatwierdzona strona przyjmująca płatności przez zatwierdzone konto to definicja problemu.
2. **Nowa linia produktów.** Konto zatwierdzono dla jednego rodzaju towarów, a teraz sprzedaje inny, zwłaszcza z kategorii objętej ograniczeniami.
3. **Przyjmowanie płatności za kogoś innego.** Firmę znajomego, dostawcy, spółki siostrzanej. To laundering w dosłownym rozumieniu zasad, bez względu na intencję.
4. **Sprzedaż dla podmiotów trzecich.** Sklep, który staje się marketplace'em, obsługuje teraz płatności innych sprzedawców, a to wymaga innego rodzaju konta.
5. **Zmieniony model biznesowy.** Przejście od sprzedaży jednorazowej do subskrypcji albo od towarów do usług zmienia ryzyko, które dostawca zatwierdził.
6. **Afilianci i odsprzedawcy.** Partnerzy kierujący klientów na strony, których dostawca nigdy nie widział.

Jak trzymać się od tego z daleka

- **Jedna zatwierdzona działalność na konto.** Jeśli klientowi opisałybyś ją jako inną firmę, potrzebuje własnego zatwierdzenia.
- **Poinformuj dostawcę, zanim coś zmienisz.** Nowe strony, produkty, kraje i modele rozliczeń. Większość jest zatwierdzana po krótkiej ocenie, a wszystkie wyglądają znacznie gorzej, gdy zostaną wykryte.
- **Nigdy nie użyczaj konta.** Ani po znajomości, ani za opłatą.
- **Dbaj o prawdziwy deskryptor.** Nazwa na wyciągu powinna prowadzić do strony, na której klient kupił.

- **Wiedz, co robią twoi partnerzy.** Merchant odpowiada za ruch, który kierują do niego afilianci.

Jeśli dostawca podniesie tę kwestię

Odpowiedz szybko i w pełni. Wyjaśnij, czym były transakcje, pokaż strony, których dotyczą, i powiedz, co zmieniono. Niezgłoszony drugi sklep wyjaśniony pierwszego dnia to korekta zgodności. Te same fakty przyznane po tygodniu milczenia wyglądają jak zatajenie i dostawca musi je tak potraktować.

Dla dostawców i ISO

Wzorzec stojący za większością prawdziwych przypadków to wniosek nieco zbyt czysty: prosty sklep niskiego ryzyka, nowa domena, mały ruch i wolumen napływający szybciej, niż strona mogłaby to wyjaśnić. Najwięcej czasu zabierają uczciwe przypadki opisane wyżej. Pytanie przy onboardingu o inne strony, marki i planowane zmiany usuwa wiele z nich, zanim się zaczną.

Źródła

- [LegitScript: podstawy BRAM i VIRP](#) (po angielsku)
- [Onlayer: czym jest transaction laundering i jak się go wykrywa](#) (po angielsku)

Czytaj online: <https://payments-marketplace.com/pl-PL/insights/transaction-laundering/>

Payments Marketplace Ltd

Registered in England & Wales No. 17424288

Garden Ctg, Dereham Road, Dereham, Norfolk, NR19 2PW, UK

connect@payments-marketplace.com · +44 1366 727140